MISE EN PLACE D'UNE LIVEBOX AVEC DOUBLE NAT SOUS LINUX

Table des matières

I/ Configuration de la Livebox

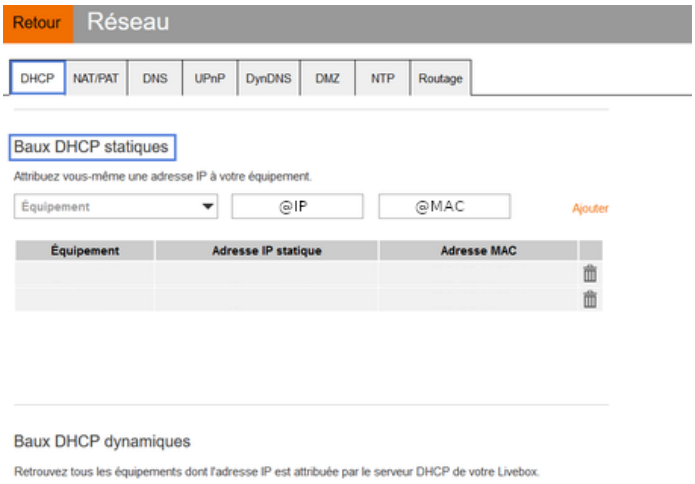
- Se connecter sur la Livebox avec le mot de passe indiqué
- Dans **Réseau** → **DHCP**, modifier l'adresse IP de la Livebox ainsi que son masque, la passerelle et la plage DHCP si besoin pour correspondre aux besoins.

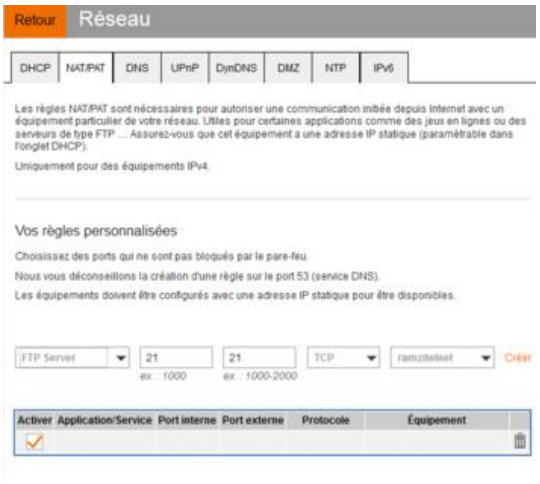
II/ Mise en place des règles de routage NAT

(Pour des raisons de sécurité, il m'a été demandé de ne pas mettre de captures d'écrans concernant la configuration de la Livebox)

- Ajouter les équipements (ici des VPN) avec une adresse statique choisie dans **Réseau** → **DHCP** → **Baux statiques**
- Dans **NAT/PAT**, ajouter une règle correspondant à l'équipement voulu avec les bons ports ainsi que le nom de l'équipement. Le type d'application/service peut être renseigné à la main avec **Nouveaux** dans la première case
- Une fois la règle choisie rentrée, créer la règle et vérifier son fonctionnement.

/!\ Attention aux ports lors de l'ajout de la règle avec les ports internes et externes.





III/ Mise en place du routage avec les deux sorties différentes

- Sous Linux, il faut créer des tables virtuelles au sein des VPNs pour le double routage
- Pour créer la table : **nano /etc/iproute2/rt_tables** → rajouter le nom de la table avec le numéro de table ainsi que son nom dans le fichier
- Dans le fichier **/etc/network/interfaces**, rajouter une nouvelle connexion possible avec une nouvelle carte ainsi que son masque (sans passerelle).
- Ajouter les règles nécessaires avec comme syntaxe : **up ip rule add *SELECTOR ACTION* || true**
  → Le **|| true** permet d'exécuter les commandes suivantes même si la ligne en question émet des erreurs
- Vérifier le bon ajout des règles ip rule avec un **ip rule list**
- Ajouter si besoin une règle avec **iptables** pour gérer le passage des paquets au sein du pare-feu

IV/ Problèmes rencontrés et solutions

- La sortie prise par les paquets ne sont pas les sorties voulues (lié à openvpn et UDP → bug)
  → Forcer l'utilisation de l'IPv4 en modifiant une ligne dans le fichier de conf serveur : **proto udp** → **proto udp4**
  → Ajouter dans le fichier de conf du serveur la ligne **multihome**

V/ Tests

Afin de vérifier si le VPN fonctionne bien et prend bien la route choisie, les tests suivants ont été effectués

- **ping @*IP* VPN** → Le ping a permis de vérifier s'il y avait une réponse venant des VPNs
- **ping -I *interface* @*VP*** → Permet de choisir l'interface par laquelle passer
- **ip route show** → Vérifier que la table a bien été prise en compte
- **ip rule show** → Vérifier que les règles de routage ont bien été appliquées
- **iptables -L** → Lister les règles de pare-feu existantes pour assurer le passage des paquets
- Essayer de se connecter au VPN pour voir si cela fonctionne
- Vérifier le fichier de logs avec un **tail** en **udp** → Afin de vérifier si le VPN renvoie les paquets

VI/ Final

- Redémarrer le serveur pour vérifier que toute la configuration effectuée fonctionne même après un redémarrage